The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
10/23/2019

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Firefox Extended Support Release (ESR), the most severe of which could allow for arbitrary code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Firefox ESR is a version of the web browser intended to be deployed in large organizations. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Firefox versions prior to 70
- Firefox ESR versions prior to 68.2

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Firefox Extended Support Release (ESR), the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

- Heap buffer overflow in FEC processing in WebRTC (CVE-2018-6156)
- Heap overflow in expat library in XML_GetCurrentLineNumber (CVE-2019-15903)
- Use-after-free when creating index updates in IndexedDB (CVE-2019-11757)

- Potentially exploitable crash due to 360 Total Security (CVE-2019-11758)
- Stack buffer overflow in HKDF output (CVE-2019-11759)
- Stack buffer overflow in WebRTC networking (CVE-2019-11760)
- Unintended access to a privileged JSONView object (CVE-2019-11761)
- document.domain-based origin isolation has same-origin-property violation (CVE-2019-11762)
- Incorrect HTML parsing results in XSS bypass technique (CVE-2019-11763)
- Memory safety bugs fixed in Firefox 70 and Firefox ESR 68.2 (CVE-2019-11764)
- Incorrect permissions could be granted to a website (CVE-2019-11765)
- CSP bypass using object tag with data: URI (CVE-2019-17000)
- CSP bypass using object tag when script-src 'none' is specified (CVE-2019-17001)
- upgrade-insecure-requests was not being honored for links dragged and dropped (CVE-2019-17002)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by Mozilla to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2019-33/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-34/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6156
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11757
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11758
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11759
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11760
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11761
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11762
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11763
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11764
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11765
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15903
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17000
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17001

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17002

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov

DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited